Section:	06	Title:	Information Security
Sub Section:	05	Title:	Communications
Document:	04	Title:	Wide Area Network

1. STANDARD

ISD will ensure that accesses to, and use of, all ADOA networks and information are properly authorized and controlled.

1.1. Summary of Standard Changes

1.2. Purpose

To protect and secure all ISD information assets from outside threats and to maintain proper usage of all information and associated equipment.

1.3. Scope

Applies to all users, their equipment, communication devices, and the information accessed by the users.

1.4. Responsibilities

Employees will follow all established network procedures.

1.5. Definitions and Abbreviations

1.6. Description of Standard

Standard support procedures for access will be with proper justification, authorization, and compliant agreements, that communications will be conducted for business related reasons only, the security controls will be consistent throughout ISD networks.

1.7. Implications

Established protective measures to ensure integrity, confidentiality, and proper usage of all ISD information are mandatory. Hardware will be used only for authorized job functions and physical security procedures will be followed.

1.8. References

1.9. Attachments

2. ADMINISTRATIVE PROCEDURES

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. Configurations and set-up parameters on all client hosts attached to ISD networks will comply with in-house security management policies and standards.

2.2.2. Systems handling sensitive, valuable, or critical information will securely log all significant security relevant events such as password guessing attempts, attempts to use unauthorized privileges, modifications to production software, or system software, etc.

2.2.3. All inbound dial-up lines connected to ISD internal networks and/or multi-user systems will pass through access control points (firewalls both physical and software) before reaching log-in status.

2.2.4. Controls and monitoring devices will be used to ensure that all equipment and software as used according to established practices and not for unauthorized purposes.

2.2.5. ISD will reserve the right to terminate network connections with third party systems upon not meeting ISD security measures.

2.3. References

2.4. Attachments

3. LOG-IN PROCEDURES

3.1. Summary of Procedure Changes

3.2. Procedure Details

3.2.1. If three consecutive incorrect log-in attempts are made, that system ID will be suspended until reset by a system administrator.

3.2.2. Passwords will automatically by checked when created by a user to verify that the passwords contain a minimum of six characters.

3.2.3. Any unattended workstation will always by logged-off. Any system not in use for more than three minutes automatically be put in a secure screen mode.

3.3. References

3.4. Attachments

Section:	06	Title:	Information Security
Sub Section:	05	Title:	Communications
Document:	04	Title:	Wide Area Network

4. GENERAL PROCEDURES

4.1. Summary of Procedure Changes

4.2. Procedure Details

4.2.1. No software will be downloaded from other sources to ISD systems without approved security measures in place.

4.2.2. Virus checking programs approved by ISD will be in continuous use on all servers available to networked personal computers.

4.2.3. No dial-up modems will be connected to workstations that are simultaneously connected to any ISD network are allowed.

4.2.4. Any user connected to an ISD network will observe all existing ISD security procedures concerning confidentiality, information integrity, and threat avoidance.

4.3. References

4.4. Attachments